ET

INSTALLATION ET CONFIGURATION D'UNE INFRASTRUCTURE RÉSEAU SANS-FIL

AVEC

INTERFACE DE GESTION UTILISATEURS

Quentin MARACHE, Pierre-Damien WEBER, Jean-Baptiste FIRMIN

Tables des matières

Préambule

Vous êtes chargés de la création du réseau sans fil d'une petite entreprise et donc de réaliser une interface de gestion des utilisateurs WIFI. La gestion de ce réseau doit être faite par le service administratif donc par des personnes ***incompétentes en informatiques car*** il n'y aura pas d' administrateur/Ingénieur réseau qui se chargera de créer/supprimer les comptes.

L'installation du serveur d'authentification Radius, la configuration des bornes Wifi avec la norme WPA2 (802.1X/EAP) ainsi que le stockage du mot de passe dans un annuaire LDAP doit être transparent pour l'entreprise mais doit aussi se faire au prix le plus bas.

De plus vous devez créer un site internet de gestion des utilisateurs afin de faciliter la gestion des utilisateurs au service administratif ,ce formulaire Web permet la gestion des utilisateurs, tout en s'occupant de la création des comptes, des sessions (login + mdp) ,la date de création, la date d'expiration, et la fermeture du compte lors de l'expiration avec toutes les communications réseaux requises.

I. Fonctionnement générale du projet

L'architecture réseau déployée dans ce projet s'appuie et fonctionne avec plusieurs protocoles :

- 802.1X est le standard de la norme IEEE
- WPA2 est un mécanisme pour sécuriser les réseaux sans-fil
- EAP est un mécanisme d'identification universel
- RADIUS est un protocole d'authentification standard

A. Connexion interface Annuaire

Dans un premier temps, il faut se connecter sur l'interface d'annuaire https://192.168.1.50
Une fois connecté sur la page d'administration de l'annuaire, dans notre cas il s'agit d'un annuaire libre « OpenLdap », il est demandé ensuite de créer un utilisateur avec les champs suivants :

- Nom Prénom et Mot de passe du compte
- UID (il s'agit du n° identifiant sur la base LDAP)
- Types d'organisations (user ou compagnie)
- Date d'entrée et date d'expiration
- Autorisation « DialUpAccess » (accès Internet)

B. Les protocoles et leurs fonctionnements

802.1X

Le standard **802.1x** est une solution de sécurisation, mise au point par l'IEEE en juin 2001, permettant d'authentifier (identifier) un utilisateur souhaitant accéder à un réseau (filaire ou non) grâce à un serveur d'authentification.
Le 802.1x repose sur le protocole EAP (Extensible Authentication Protocol), défini par l'IETF, dont le rôle est de transporter les informations d'identification des utilisateurs

EAP

Le fonctionnement du protocole **EAP** est basé sur l'utilisation d'un contrôleur d'accès, chargé d'établir ou non l'accès au réseau pour un utilisateur. Le contrôleur d'accès est un simple garde-barrière servant d'intermédiaire entre l'utilisateur et un serveur d'authentification, il ne nécessite que très peu de ressources pour fonctionner. Dans le cas d'un réseau sans fil, c'est le point d'accès qui joue le rôle de contrôleur d'accès.

WPA2

La norme IEEE 802.11i (ou WPA2) fournit un chiffrement plus élaboré que celui de la solution intérimaire WPA (Wi-Fi Protected Access).

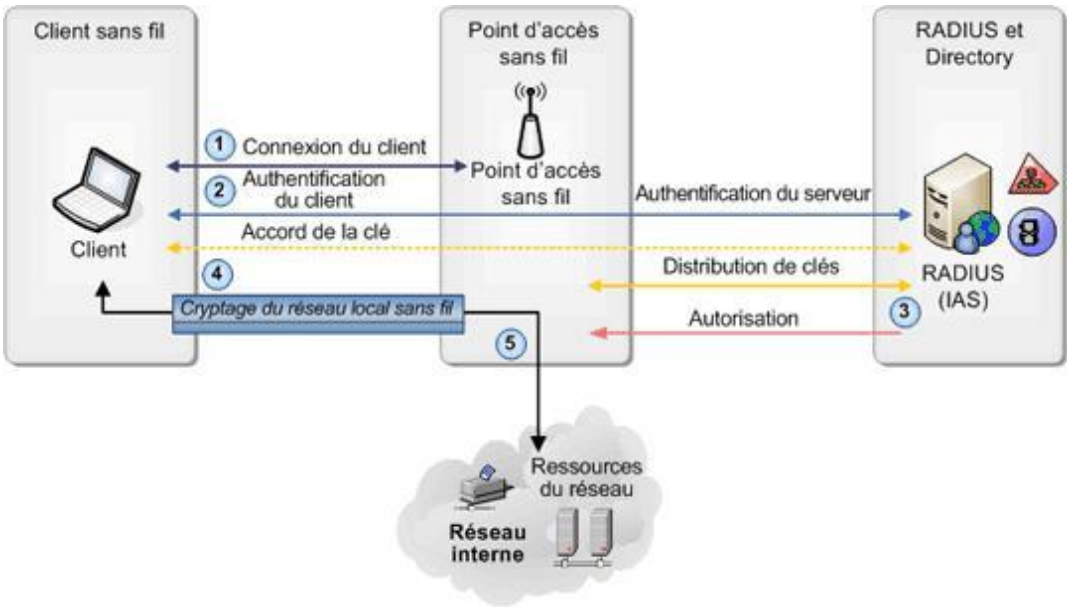
En particulier, la norme WPA2 impose le support d'un chiffrement basé sur AES. Ce protocole est considéré comme complètement sécurisé.

Radius

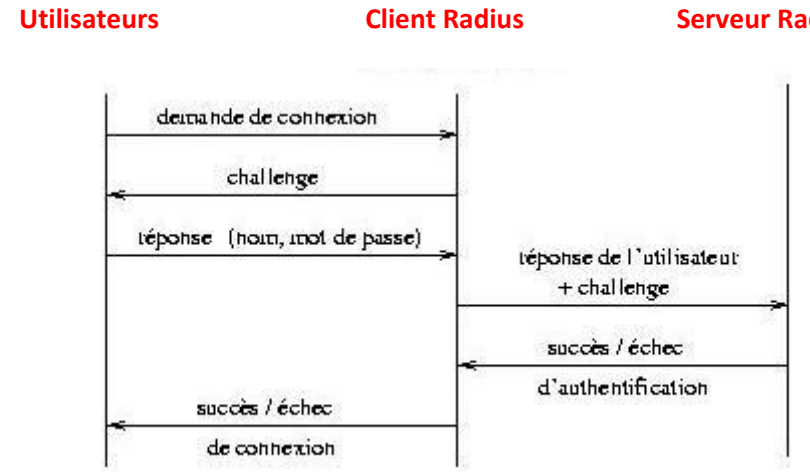
Le fonctionnement de **RADIUS** est basé sur un système client/serveur chargé de définir les accès d'utilisateurs distants à un réseau. Il s'agit du protocole de prédilection des fournisseurs d'accès à Internet car il est relativement standard et propose des fonctionnalités de comptabilité permettant aux FAI de facturer précisément leurs clients.

Le protocole RADIUS repose principalement sur un serveur (FreeRadius), relié à une base d'identification (annuaire OpenLdap) et un client RADIUS, appelé NAS (Borne Wifi), faisant office d'intermédiaire entre l'utilisateur final et le serveur. L'ensemble des transactions entre le client RADIUS et le serveur RADIUS est chiffrée et authentifiée grâce à un secret partagé.

Son fonctionnement :

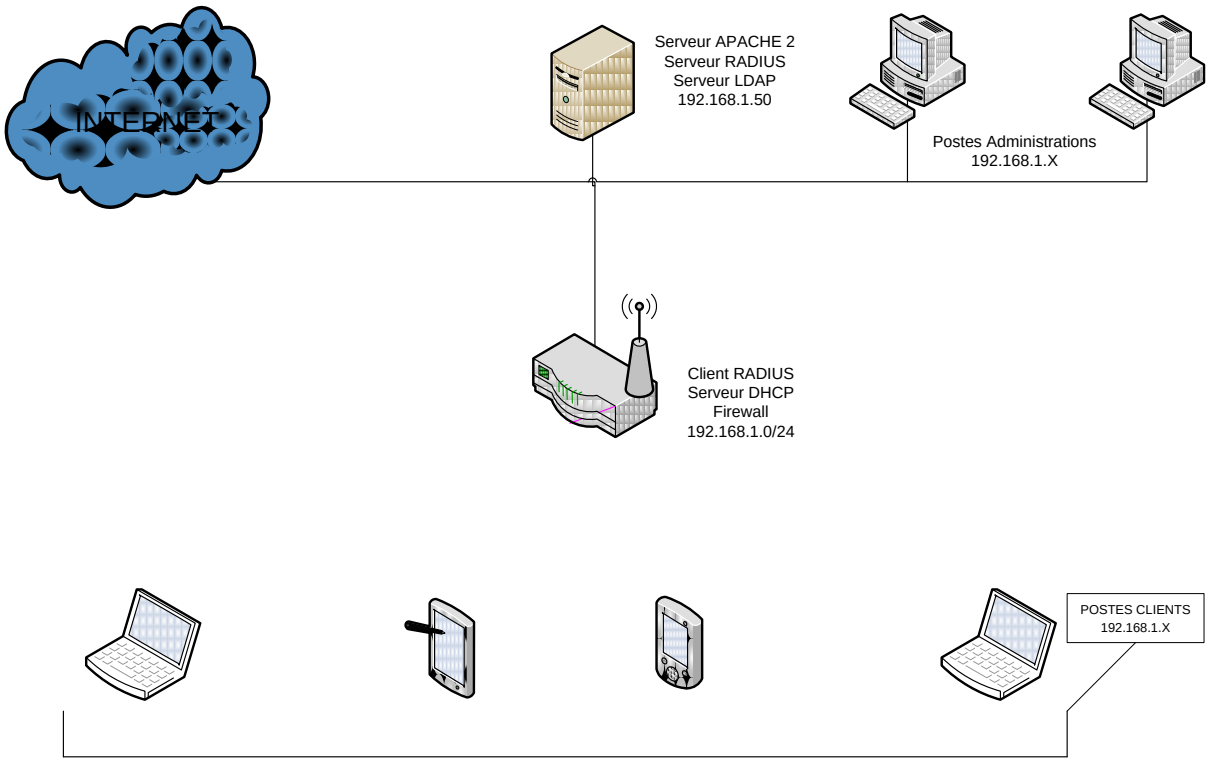


C. Phases de connexions



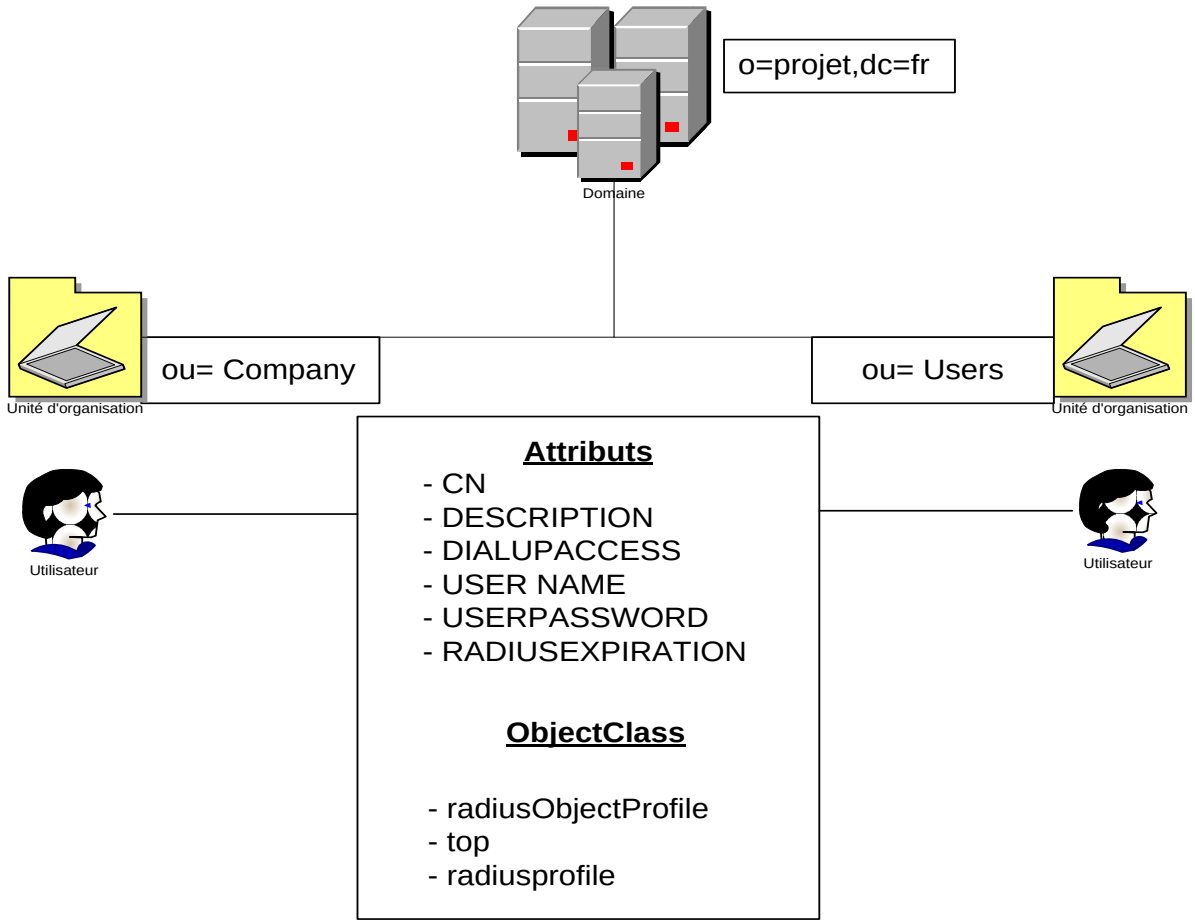
D. Schéma D'architecture du domaine « Projet.fr »

1. Plan d'adressage IP



Le réseau FreeRadius fonctionne grâce a l'architecture réseau ci-dessus, il permet de d'offrir une connectivite Wifi sécurisé à toute une gamme d'équipement compatible aux normes Wifi - Alliance.

2. Schéma de l'annuaire LDAP



Dans l'annuaire LDAP, nous avons défini plusieurs attributs qui nous permettent de communiquer avec le serveur Radius :

- CN : Nom et prénom de la personne
- DESCRIPTION : Date d'entrée de la personne
- DIALUPACCESS : permet d'autoriser ou non l'accès a internet pour l'utilisateur
- USER NAME : définit le login de la personne
- USERPASSWORD : définit le mot de passe de la personne
- RADIUSEXPIRATION : définit la date d'arrêt d'accès à Internet.

Nous avons besoins de trois « Objetclass » pour que les utilisateurs soient reconnus par le schéma.

- RadiusObjectProfile
- Top
- Radiusprofile

II. Mise en place du projet

A. Installation et configuration du LDAP

1. Installation du service LDAP

Entrer la commande suivante pour installer OpenLDAP sur la DEBIAN:

>> **apt-get install slapd + apt-get install ldap-utils**

Une fois l'application installé, l'ensemble des fichiers se trouvent dans /etc/ldap. Faire une sauvegarde du ldap.conf et slapd.conf dans le même répertoire (etc/ldap) en rajoutant « .sav »

2. Configuration du service OpenLDAP

Configuration du fichier « **slapd.conf** », ce fichier contient les modèles Nommages de sécurité ainsi que les Access listes .

Mettre les includes :

```
include         /etc/ldap/schema/core.schema
include         /etc/ldap/schema/cosine.schema
include         /etc/ldap/schema/nis.schema
include         /etc/ldap/schema/inetorgperson.schema
include         /etc/ldap/schema/freeradius.schema
```

- Ajouter la ligne: `allow bind_v2`
- Modifier le suffix: `suffix "o=projet,dc=fr"`
- modifier le login administrateur: `rootdn "cn=admin,o=projet,dc=fr"`
- Ajouter le mot de passe en clair ou en crypté: `rootpw secret` ou entrer la commande slappasswd puis recopier le mot de passe crypté
- Paramétrer l'accès de l'écriture de la base (ACLs):

```
access to attrs=userPassword,shadowLastChange
        by dn="cn=admin,o=projet,dc=fr" write
        by * none

access to dn.base="" by dn="cn=admin,o=projet,dc=fr" write

access to *
        by dn="cn=admin,o=projet,dc=fr" write
        by * none
```

Redémarrer le serveur slapd avec la commande >> **/etc/init.d/slapd restart**

Faire un test de configuration >> **ldapsearch -x -b "o=projet,dc=fr" "objectclass=*"**

3. Peuplement de l'annuaire

Ajout de la racine dans le fichier **racine.ldif** :

```
dn:  o=projet,dc=fr
objectClass: dcObject
objectClass: organization
o: projet
dc: fr
```

Entrer la commande pour ajouter la racine >> **ldapadd -x -D "cn=admin,o=projet,dc=fr" -W -f racine.ldif**

Commande pour vérifier l'ajout: **ldapsearch -x -D "cn=admin,o=projet,dc=fr" -W -b "o=projet,dc=fr"**

Ajout du groupe dans le fichier ou.ldif

```
dn: ou=company,o=projet,dc=fr
objectClass: organizationalUnit
objectClass: top
ou: company

dn: ou=users,o=projet,dc=fr
objectClass: organizationalUnit
ou: users
```

Entrer la commande pour ajouter les organisations >> **ldapadd -x -D "cn=admin,o=projet,dc=fr" -W -f ou.ldif**

Ajout d'utilisateurs dans le fichier utilisateur.ldif

```
dn: cn=bob company,ou=company,o=projet,dc=fr
objectClass: radiusObjectProfile
objectClass: top
objectClass: radiusprofile
dialupAccess: yes
userPassword: password
structuralObjectClass: radiusObjectProfile
uid: C00001
cn: bob company
description: 15/12/09

dn: cn=alice user,ou=users,o=projet,dc=fr
cn: alice user
objectClass: radiusObjectProfile
objectClass: top
objectClass: radiusprofile
dialupAccess: yes
structuralObjectClass: radiusObjectProfile
uid: U00001
userPassword: password
radiusExpiration: "27 Aug 2010"
description: 11/12/12
```

Entrer la commande pour ajouter les utilisateurs >> **ldapadd -x -D "cn=admin,o=projet,dc=fr" -W -f users.ldif**

B. Installation et configuration de FreeRadius

Exécuter la commande suivante pour installer FreeRadius ainsi que d'autre logiciels nécessaire à son fonctionnement:
>> **apt-get install openssl libssl libssl-dev libldap2-dev g++ build-essential debian-builder libstdc++6.4-1-dev libmysqlclient15-dev**

Puis l'installer à l'aide des commandes classiques :

- **./configure**
- **make**
- **make install**

Une fois l'installation finalisée, nous pouvons tester le serveur FreeRadius sans modification nécessaire. Lancer la commande suivante: **radiusd -X**
Nous pouvons remarquer que le serveur FreeRadius fonctionne et écoute correctement:

```
/*********/

} # server
radiusd: #### Opening IP addresses and Ports ####
listen {
      type = "auth"
      ipaddr = *
      port = 0
}
listen {
      type = "acct"
      ipaddr = *
      port = 0
}
listen {
      type = "control"
 listen {
      socket = "/usr/local/var/run/radiusd/radiusd.sock"
 }
}
Listening on authentication address * port 1812
Listening on accounting address * port 1813
Listening on command file /usr/local/var/run/radiusd/radiusd.sock
Listening on proxy address * port 1814
Ready to process requests.
```

1. Configuration des fichiers du service FreeRadius

Pour ainsi mettre en place l'authentification FreeRadius, nous allons configurer certains fichiers pour que le serveur puisse communiquer avec le serveur LDAP et utiliser le protocole d'authentification souhaité.

A) Modification du fichier CLIENTS.CONF

```
/*********/


#
#  You can now specify one secret for a network of clients.
#  When a client request comes in, the BEST match is chosen.
#  i.e. The entry from the smallest possible network.
#
client 192.168.1.1 {
      secret      = freeradius
      shortname   = DLINK DIR-615

/*********/
```

Dans ce fichier nous ajoutons notre Access point pour que le serveur FreeRadius puisse communiquer avec notre NAS

B) Modification du fichier MODULES/LDAP

```
/*********/

#
ldap {
      #
      #  Note that this needs to match the name in the LDAP
      #  server certificate, if you're using ldaps.
      server = "127.0.0.1"
      identity = "cn=admin,o=projet,dc=fr"
      password = ldap
      basedn = "o=projet,dc=fr"
      filter = "(&(uid=%{%{Stripped-User-Name}:-%{User-
      Name}})(dialupAccess=yes))"
      base_filter = "(objectclass=radiusprofile)"

/*********/

      # default_profile = "cn=radprofile,ou=dialup,o=My Org,c=UA"
      # profile_attribute = "radiusProfileDn"
      access_attr = "dialupAccess"

/*********/

      #  Novell may require TLS encrypted sessions before returning
      #  the user's password.
      #
      password_attribute = userPassword

/*********/
```

Ici, nous précisons les paramètres du serveur OpenLDAP ainsi que les attributs d'authentifications

C) Modification du fichier SITE-ENABLED/DEFAULT

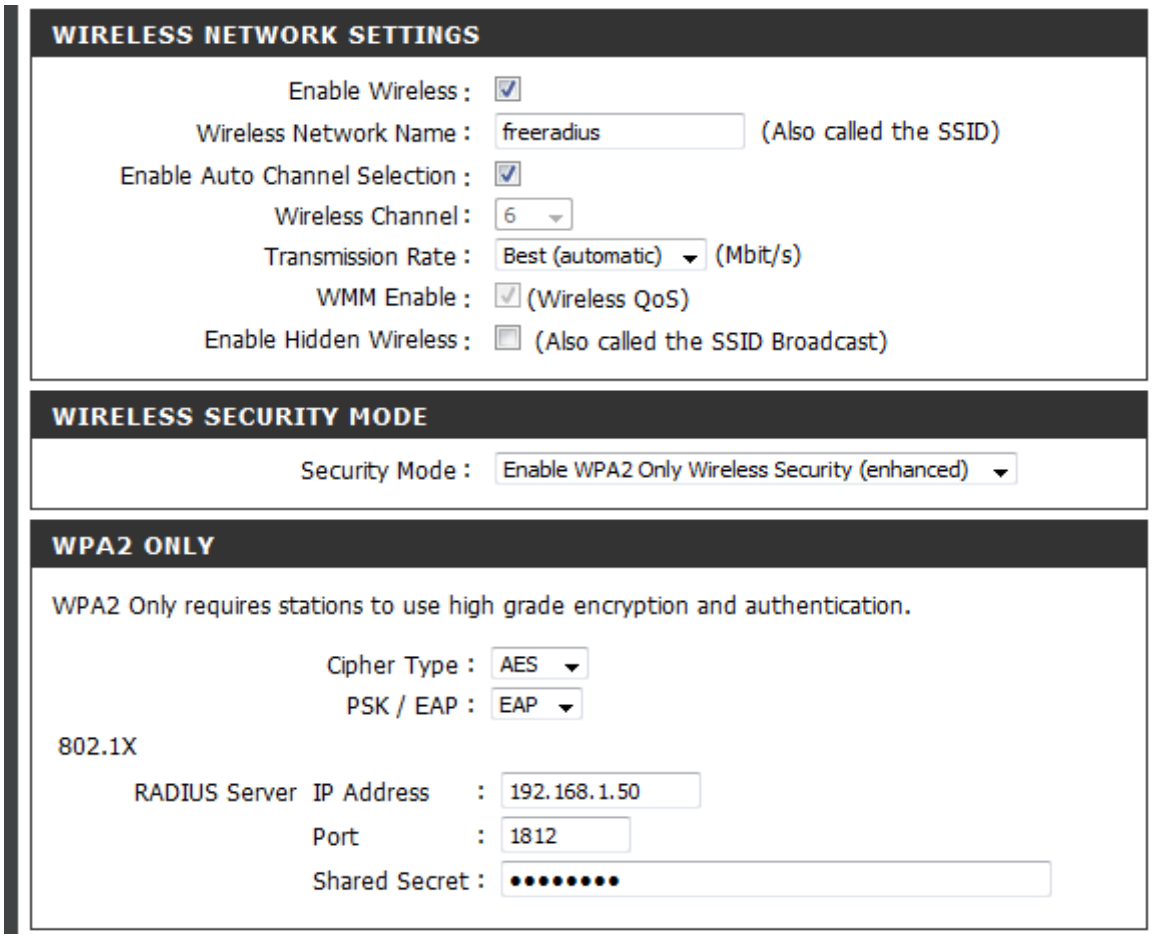
```
/*********/
#
      #  The ldap module will set Auth-Type to LDAP if it has not
      #  already been set
      ldap
/*********/
      #
      # Use the checkval module
      checkval
/*********/
      # Uncomment it if you want to use ldap for authentication
      #
      # Note that this means "check plain-text password against
      # the ldap database", which means that EAP won't work,
      # as it does not supply a plain-text password.
      Auth-Type LDAP {
            ldap
      }
      #
      #  Allow EAP authentication.
      eap
/*********/
```

D) Modification du fichier SITE-ENABLED/INNER-TUNNEL

```
/*********/
      #  The ldap module will set Auth-Type to LDAP if it has not
      #  already been set
      ldap

/*********/

      #
      # Use the checkval module
      checkval

/*********/

# Uncomment it if you want to use ldap for authentication
      #
      # Note that this means "check plain-text password against
      # the ldap database", which means that EAP won't work,
      # as it does not supply a plain-text password.
      Auth-Type LDAP {
            ldap
      }
      #
      #  Allow EAP authentication.
      eap
/*********/
```

Dans ces deux fichiers nous précisons les deux systèmes d'authentification: LDAP et EAP

2. Configuration de L'Access Point



Dans l'interface de configuration du point d'accès, renter les paramètres ci-dessus.

C. Installation et configuration du serveur Apache

1. Installation du serveur Apache version 2 et PHP 5

Lancer les commandes suivantes pour installer Apache 2 et PHP5:

>> **apt-get install apache2**

>> **apt-get install libapache2-mod-php5 php5-cli php5-common php5-cgi**

Une fois l'installation terminée lancer le navigateur internet et aller sur le localhost. Si Apache 2 fonctionne correctement, le navigateur devra afficher :"It's Works !"
Nous allons maintenant sécuriser le localhost afin que personne n'y accède. Pour cela, aller dans le répertoire d'Apache 2: /etc/Apache 2/sites-enabled et éditer le fichier 000-default:

```
<VirtualHost *:80>
	ServerAdmin webmaster@localhost

	DocumentRoot /var/www/
	<Directory />
		Options FollowSymLinks
		AllowOverride None
	</Directory>
	<Directory /var/www/>
		Options Indexes FollowSymLinks MultiViews
		AllowOverride None
			Order deny,allow
		Deny from all
	</Directory>

	ScriptAlias /cgi-bin/ /usr/lib/cgi-bin/
	<Directory "/usr/lib/cgi-bin">
		AllowOverride None
		Options +ExecCGI -MultiViews +SymLinksIfOwnerMatch
			Order deny,allow
		Deny from all
	</Directory>
```

L'option "deny from all" bloque l'accès à tout le monde.

2. Création du site interface de gestion utilisateur (projet.fr)

exécuter la commande suivant pour créer le site:

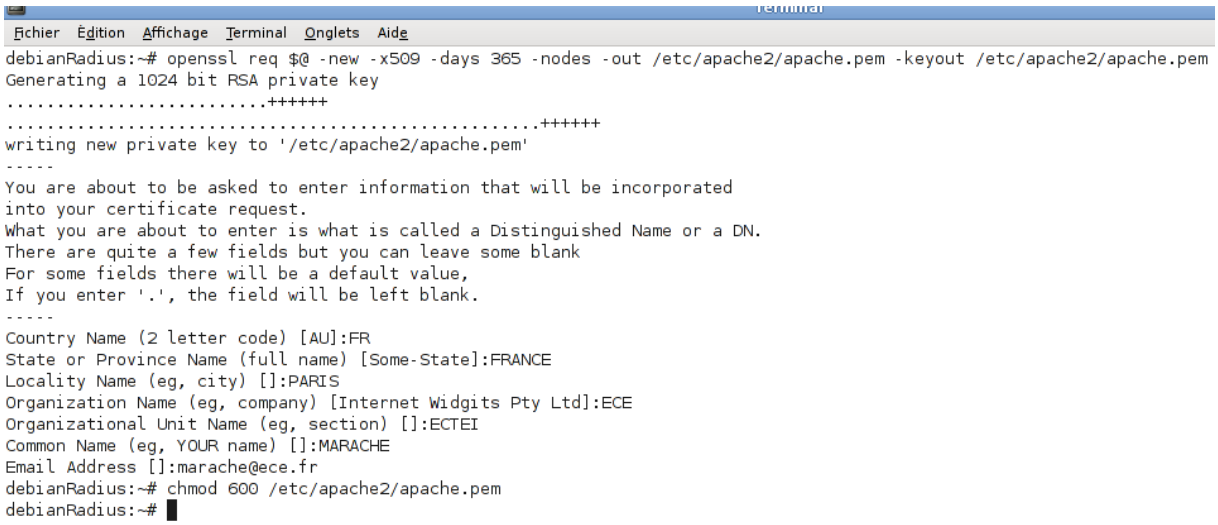
>> **a2ensite projet.fr**

La commande à créer le virtualhost projet.fr présent dans le fichier /etc/Apache 2/sites-enabled

Nous allons maintenant activer le module SSL:

>> **a2enmod ssl**

Création du certificat:



Commençons par éditer le virtualhost projet.fr:

NameVirtualHost 192.168.1.50:443

```
<VirtualHost 192.168.1.50:443>
      ServerAdmin marache@ece.fr
      ServerName www.projet.fr
      DocumentRoot /var/www/projet.fr

      SSLEngine on
      SSLCertificateFile /etc/apache2/apache.pem
      <Directory />
            Options FollowSymLinks
            AllowOverride all
      </Directory>
      <Directory /var/www/projet.fr>
            Options Indexes FollowSymLinks MultiViews
            AllowOverride all
            Order allow,deny
            allow from all
      </Directory>
</VirtualHost>
```

Dans ce fichier, nous avons précisé le port de connexion https (443) ainsi que le lien du certificat. Les ACL sont configurées par défaut.

Nous pouvons dorénavant nous connecter sur l'interface de gestion en mode sécurisé.
Pour plus de sécurité, nous allons construire un outil d'authentification du type .htaccess:

```
AuthName "Acces Restreint"
AuthType Basic
AuthUserFile "/home/debradius/user.htpasswd"
<LIMIT GET POST>

Require valid-user
</LIMIT>
```

Il suffit de placer ce fichier à la racine du répertoire du site projet.fr. Il nous faut maintenant créer des utilisateurs. Exécuter la commande suivante: **htpasswd -c .htpasswd Administrateur**

Avec "administrateur", le nom de votre utilisateur. Une fois la commande rentré, vous allez pouvoir configurer son mot de passe.

Placer ce fichier dans le répertoire de votre choix mais ne pas oublier de référencer son lien de le fichier .htaccess.

III. Mise en œuvre

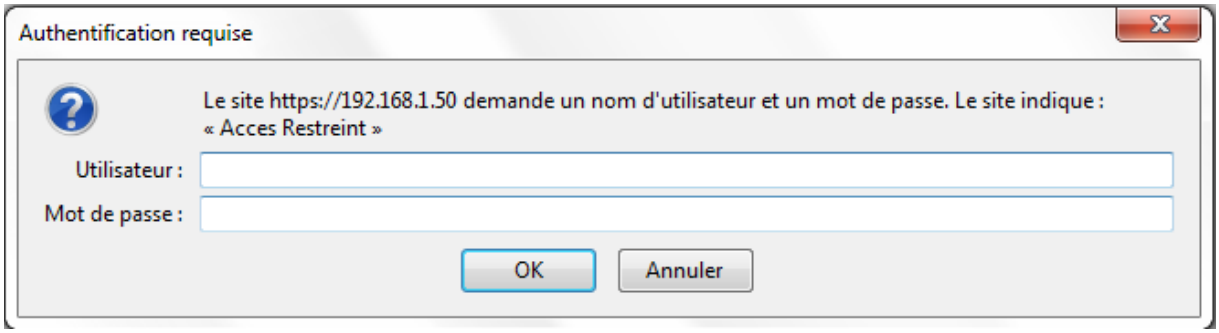
A. Procédure de gestion des comptes wifi

Afin d'aider au mieux les personnes du service administratif, elles se connectent sur l'interface de gestion des utilisateurs du réseau Wifi « freeradius » , une procédure simple et la portée de tous est crée afin d'expliquer comment se connecter et s'authentifier à partir d'un poste de l'administration, ainsi que les bases du fonctionnement d'une création, modification ou suppression d'un compte utilisateur sur l'interface Web . Cette interface de gestion est conçue pour faciliter au maximum les changements sur les comptes pour l'administrateur.

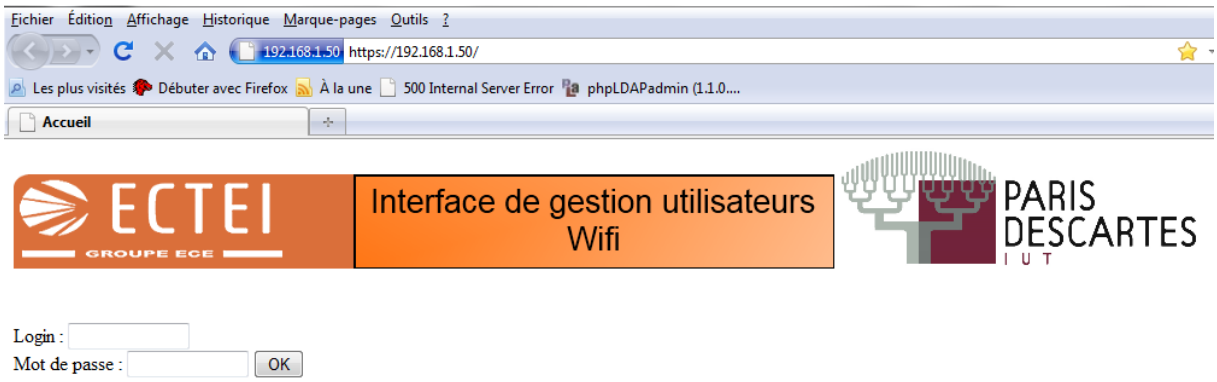
- Tout d'abord la connexion a l'interface Web du serveur :

Ouvrir le navigateur du poste puis écrire dans l'URL, le lien https:// 192.168.1.50

Accepter le certificat d'authentification du serveur qui vous est proposé, puis une demande d'authentification du serveur s'ouvre comme l'illustre l'image ci-dessous, ouvrir une session a l'aide du nom de l'utilisateur et de son mot de passe.

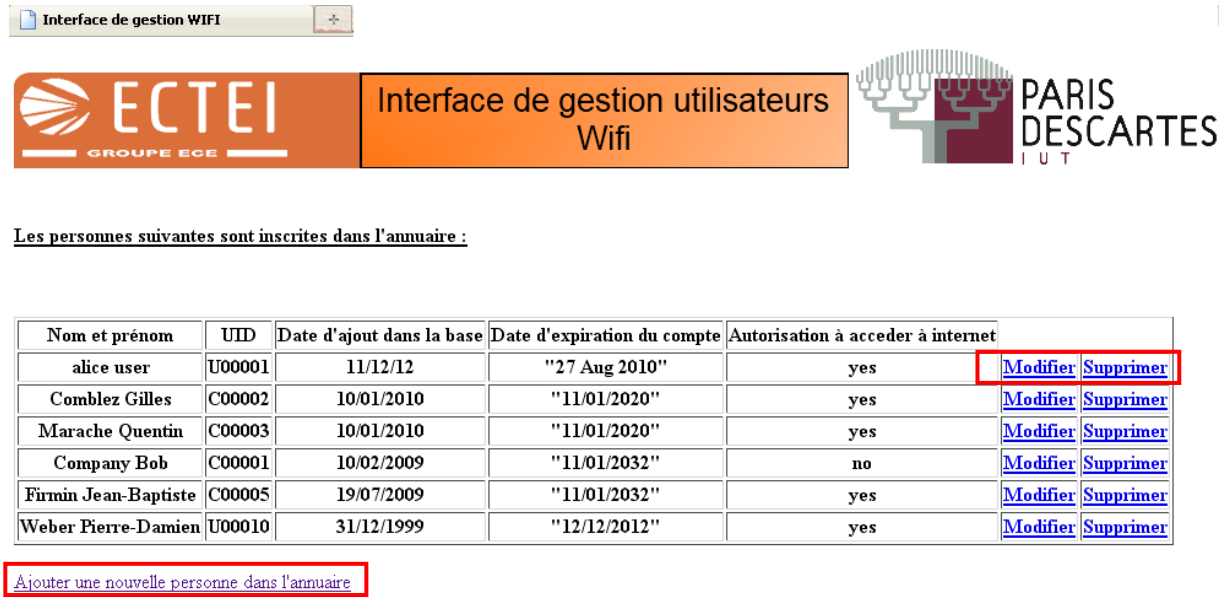


Une fois l'ouverture de session de l'administrateur ouverture, la fenêtre d'interface de gestion s'annonces, une deuxième authentification est nécessaire pour entrer sur l'annuaire de gestion. Entrer le « Login » puis le mot de passe et valider sur la touche « Ok »



L'interface de gestion est maintenant accessible, une liste des comptes utilisateur créer est affichées. Celle –ci permet de vérifier les principaux paramètres de connexions des comptes comme le nom et prénom de l'utilisateur, son identifiant « UID », la date d'ouverture et d'expiration de son compte, ainsi que le droit d'accès à Internet.

Afin de permettre une gestion plus rapide des comptes, l'interfaces contient des liens pour créer un nouvelle utilisateur dans la l'annuaire, modifier ou supprimer le compte correspondant à la ligne comme l'est illustrée ci-dessous :

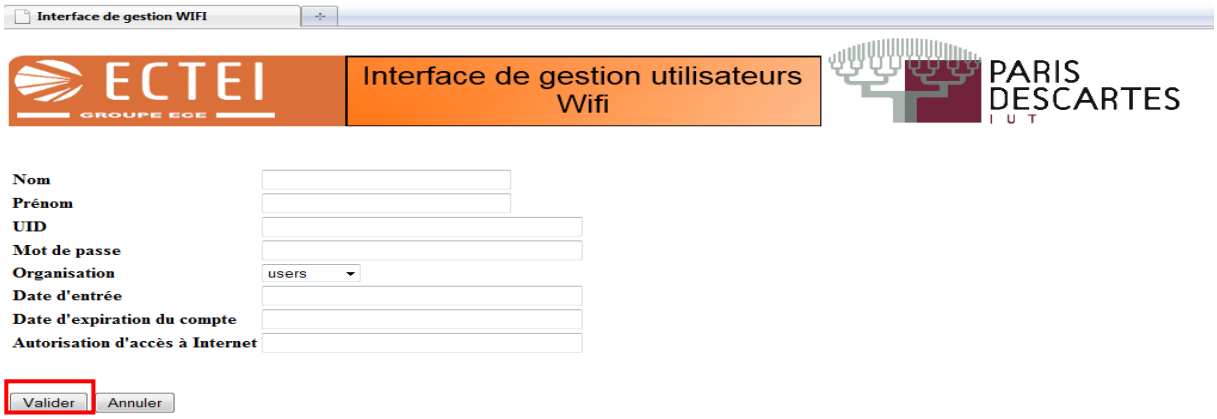


Interface de gestion des comptes utilisateurs

La création d'un utilisateur se fait en cliquant sur le lien « Ajouter une nouvelle personne dans l'annuaire » , une fenêtre s'affiche avec des paramètres obligatoire correspondant aux champs de création d'un utilisateur, chaque champs est détaillée comme tel :

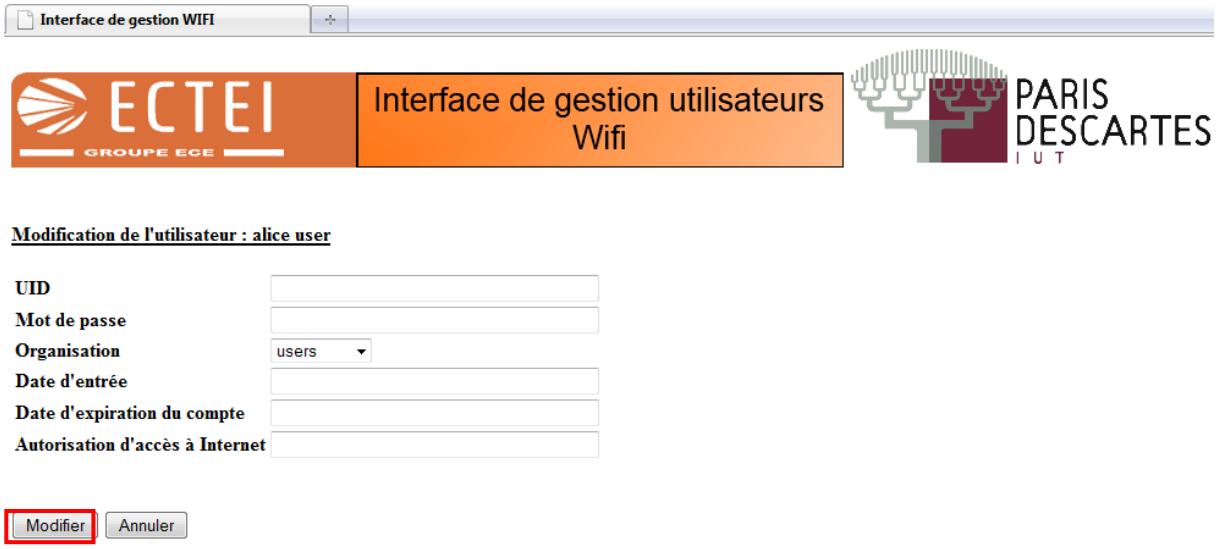
- Le nom et le prénom de l'utilisateur.
- Le UID est l'identifiant dans l'annuaire servant de login au compte pour l'ouverture d'une connexion réseau sans fil, l'utilisation d'une syntaxe permet de distinguer les utilisateurs « UxxxxX » des salariés « CxxxxX ».
- Le mot de passe est attribué par l'administrateur, il peut être personnalisable par l'utilisateur sur sa demande.
- L'organisation est un champ qui différencie les utilisateurs des salariées
- La date d'entrée est la date d'ouverture au service de connexions Wifi
- La date d'expiration du compte est la durée maximum d'utilisation du compte, une syntaxe est recommandée pour ce champ, mettre des guillemets autour de la date.
- L'autorisation d'accès à Internet est un champ qui permet de donner le droit d'accéder à Internet via la connexion réseau de « freeradius », mettre comme syntaxe « Yes » ou « No ».

Cliquer sur « Valider » pour poursuivre l'enregistrement.



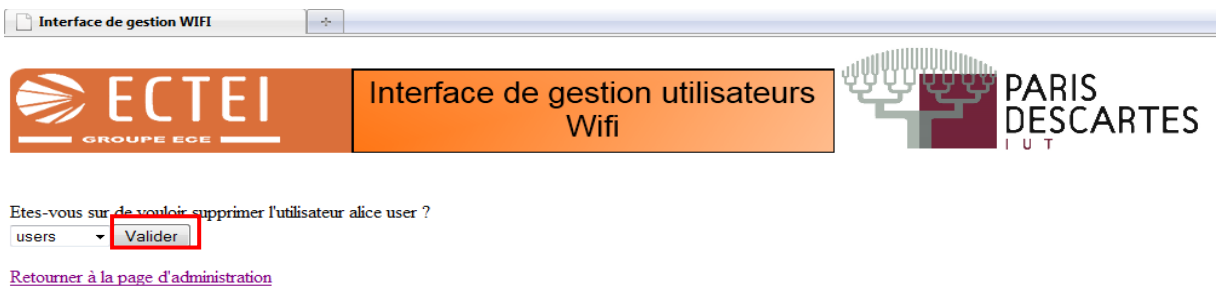
Fenêtre de création d'un compte utilisateur

La modification du compte par l'administrateur se fait sur la ligne correspondant au compte a modifier (voir l'encadrer plus haut) un clique sur le lien modifier permet d'afficher une fenêtre avec les paramètres de connexions du compte. La modification des paramètres souhaités s'effectue sur les champs voulus, le respect de la syntaxe est identique a celle de la création des comptes est conseillé pour éviter les erreurs, puis cliquer sur « Modifier » pour poursuivre l'enregistrement.



Fenêtre de modification d'un compte utilisateur

La suppression d'un compte est identique à celle de la modification, seulement le lien « supprimer » doit être sélectionné sur la ligne du compte à supprimer, une nouvelle fenêtre s'annonce avec le nom et prénom du compte à supprimer. Vérifier que le compte à supprimer est bien celui qui est souhaité puis cliquer sur « Valider » pour continuer la suppression.



Fenêtre de suppression d'un compte utilisateur

Pour conclure cette procédure, les changements sur les comptes sont du rôle du service qui gère l'administration des utilisateurs Wifi du site, aussi leur connaissance sur la gestion des utilisateurs se limite à cette procédure et au respect des règles de syntaxe des champs.
Toute autre gestion doit se faire par les personnes compétentes dans l'installation dans l'implémentation de services informatiques.

B. Procédure d'une ouverture de session pour un utilisateur

Afin d'aider au mieux les utilisateurs du réseau Wifi dont le SSID est « freeradius » , une procédure simple et la portée de tous est crée afin d'expliquer comment se connecter et s'authentifier à partir de leurs poste en quelque clique, aussi les connaissances nécessaire à la création d'une connexion est à la portée de tous . Cette procédure se veut simple et facile de compréhension pour un utilisateur, seul le pré-requis d'une demande d'accès au réseau n'est pas prise en comptes dans cette procédure.

Dans un premier temps, sélectionner le réseau « freeradius » dans la console de gestion des réseaux sans-fil disponible comme illustrer ci-dessous :

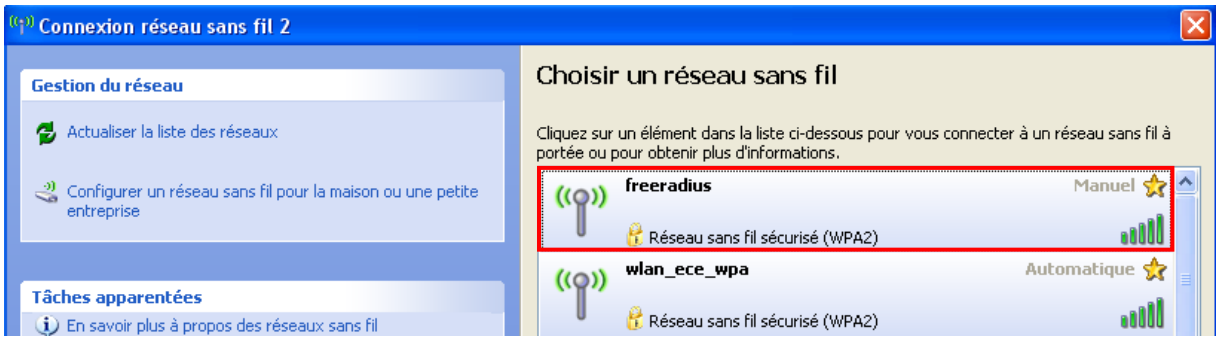
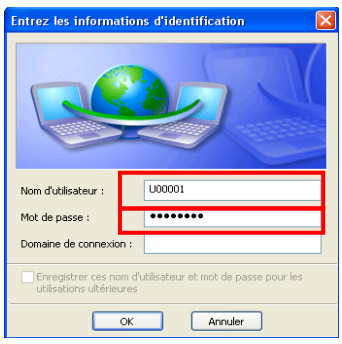


Illustration de la console de gestion des réseaux sans-fil disponible

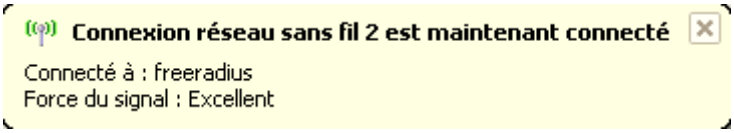
Dans un deuxième temps, une fois sélectionner le réseau sans fil, une fenêtre d'identification s'affiche avec comme champs disponible le nom d'utilisateur, le mot de passe et le domaine. Pour vous identifier au réseau « Freeradius » effectuer la correspondance des champs comme indiquer ci-dessous :

- **Nom d'utilisateur :** l'identifiant « UID » remis par les services administratifs du réseau.
- **Mot de passe :** le mot de passe remis par les services administratif du réseau.
- **Domaine :** le champ domaine n'est pas à préciser, il doit rester nul.

L'illustration ci-dessous nous montre comment remplir les champs :



Dans un dernier temps, une fois les champs remplis, la confirmation de la connexion est visible sur votre bureau grâce a une fenêtre de connexion comme illustrer ci-dessous :



Confirmation de la connexion au réseau sans fil « freeradius »

C. La vérification des paramètres réseau d'une connexion

Avant tout, l'utilisateur de la connexion doit être enregistre dans l'annuaire LDAP, il doit aussi lui être remis un login et un mot de passe de connexions par les services administratifs comme l'illustre le schéma ci-dessous :

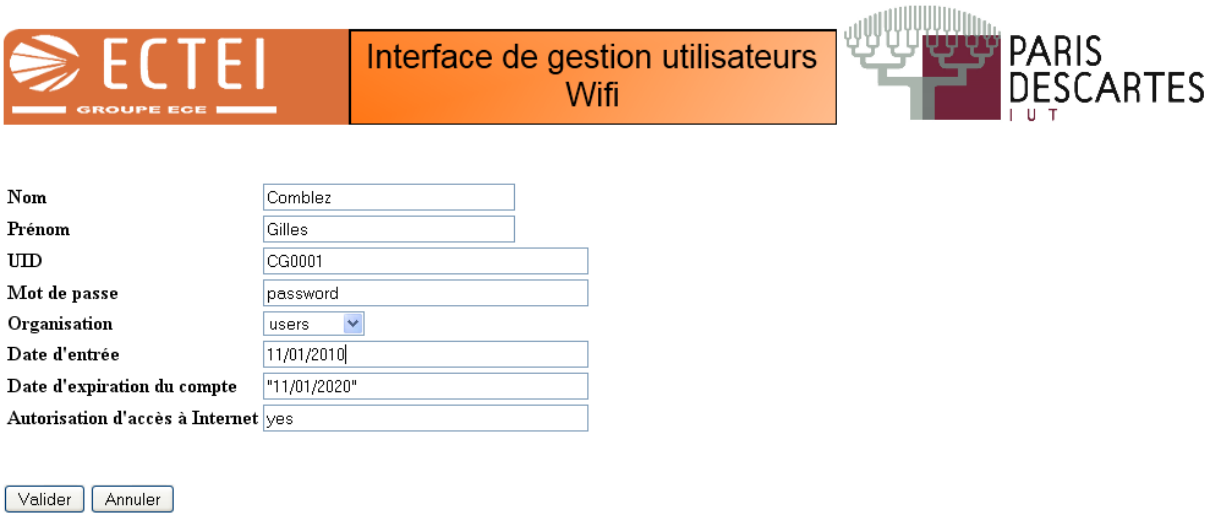
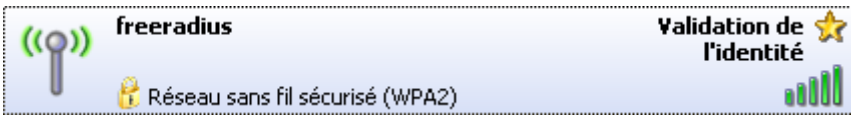


Illustration d'une création de compte sur l'interface de gestion des utilisateurs Wifi

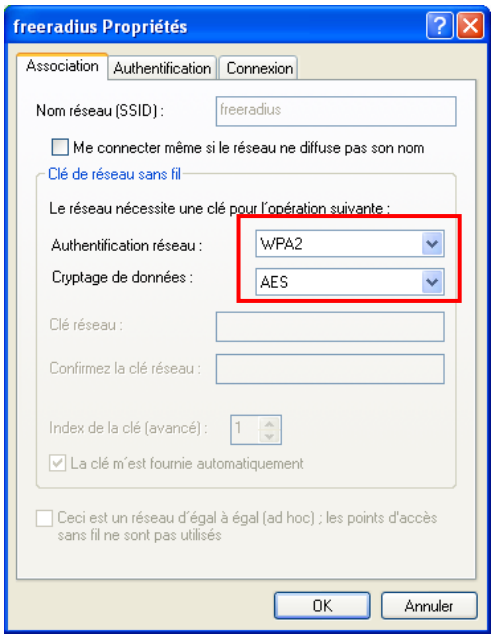
De plus la connexion au SSID « Freeradius » doit ce faire à la portée de sa zone d'émission de celui-ci afin de pouvoir se connecter.

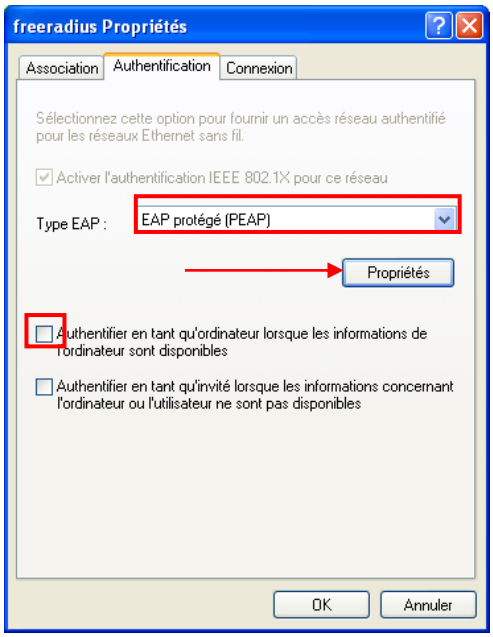


L'antenne Access Point du réseau « freeradius » est configurer pour attribuer dynamiquement la configuration TCP/IP requise pour un utilisateur, ce dernier doit avoir une configuration IP attribué dynamiquement dans ses propriétés de protocoles Internet (TCP/IP).

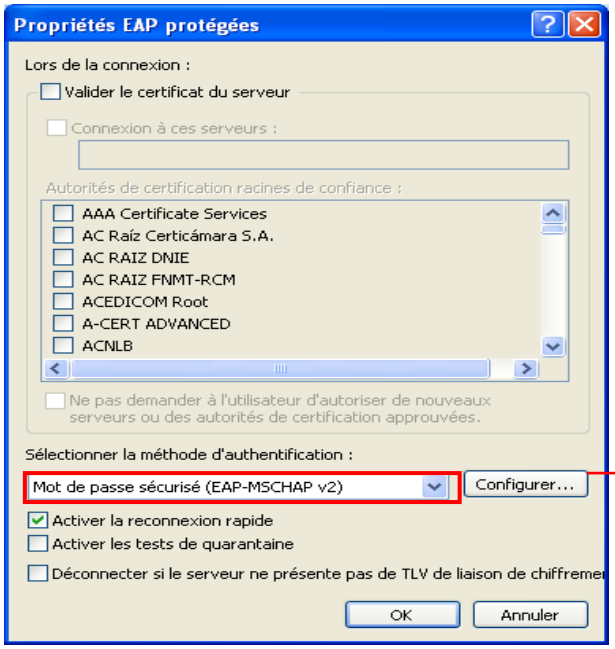
Les propriétés de configuration du réseau « freeradius » sont vérifiable sur le poste de utilisateur qui souhaite avoir une connexions sur le réseau wifi, pour cela ouvrir les paramètres de connexions réseau sans fil puis dans les propriétés du « freeradius » , comme l'illustre les schémas ci-dessous , les paramètre d'authentification du réseau sont « WPA2 » , et les paramètres de cryptages des données sont « AES » .

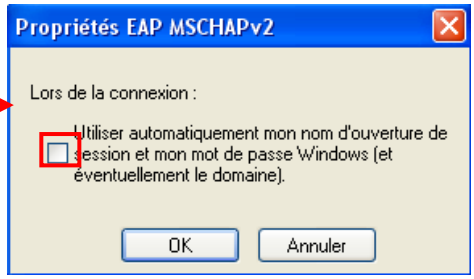
Dans l'onglet authentification, vérifier si le type « EAP » est sur le champs « EAP protégé (PEAP) », décocher la 1er coche « authentifier en tant qu'ordinateur lorsque les informations de l'ordinateur sont disponibles », puis cliquer sur propriétés pour vérifier l'authentification du type « EAP ».





Dans les propriétés EAP protégées, il faut décocher le champ « valider le certificat du serveur » , vérifier la méthodes d'authentification EAP qui doit être « EAP-MSCHAP v2 » , puis cliquer sur configurer afin de décocher le champs inclus .





Une fois c'est paramètres de connexions sans fil vérifié, lancer une ouverture de session sur le réseau « freeradius » comme expliqué dans « La procédure d'une ouverture de sessions d'un utilisateur »

D. L'analyse des étapes de connexions

La supervision des registres de connexions sur le serveur permet vérifier si un utilisateur réussit a se connecter ou non. Il permet aussi de vérifier comment il se connecte et avec quel identification ainsi que la vérification de sa réussite ou de son échec. Pour cela il y a différente étapes d'enregistrement comme expliquer dans le fonctionnement général du projet, nous nous intéresserons principalement aux étapes d'une connexion d'échec auprès du serveur radius, aux étapes d'une connexion réussit, et toute deux avec l'étape intermédiaire de la recherche dans la base LDAP.

Tout d'abord l'étapes du serveur Radius avec l'échec d'une connexions pour l'utilisateur « testderejet » , afin de montrer la pertinence d'authentification avec un serveur Radius :

- La première étape est un « **Access-Request** » qui contient l'identité de l'utilisateur qui se connecte :

```
rad_recv: Access-Request packet from host 192.168.1.1 port 3072, id=119,
length=201
      User-Name = "testderejet"
      NAS-Port = 0
      Called-Station-Id = "00-26-5A-B2-23-2C:freeradius"
      Calling-Station-Id = "00-13-02-AB-FD-0A"
      Framed-MTU = 1400
      NAS-Port-Type = Wireless-802.11
      Connect-Info = "CONNECT 11Mbps 802.11b"
      EAP-Message =
0x020800271900170301001c5fbf48fb08c57965f7f06e367428734fdd488d6d5ddd92e1a14
470c2
      State = 0x1df97e3c1bf167a899cd860936c71b6a
      Message-Authenticator = 0x9656a45e38e827840a482860b15cdf75
```

- La réponse de la base d'authentification LDAP après une verification dans sa base :

```
[ldap] performing search in o=projet,dc=fr, with filter (uid=testderejet)
[ldap] object not found
[ldap] search failed
[ldap] ldap_release_conn: Release Id: 0
[ldap] returns notfound
```

- Un « **Access-Reject** » est émis par le serveur radius pour spécifier au client que sa requête est rejetée :

```
. Sending Access-Reject of id 119 to 192.168.1.1 port 3072
      EAP-Message =
0x0109003c19001703010031959362299 01c857a5391efa75c932ef72b6cd8293aada68a846
cd19b223bdafce7b7bd9e313752fd540d79e1f62c71da13
      Message-Authenticator = 0x00000000000000000000000000000000
      State = 0x1df97e3c1af067a899cd860936c71b6a
Finished request 97.
```

Voici les différentes étapes qui sont renvoyée par le serveur Radius pour accepter la requête du client « U00001 » après l'interrogation de sa base d'authentification :

- La première étape est un « **Access-Request** » qui contient l'identité de l'utilisateur qui se connecte :

```
rad_recv: Access-Request packet from host 192.168.1.1 port 3072, id=131,
length=186
      User-Name = "U00001"
      NAS-Port = 0
      Called-Station-Id = "00-26-5A-B2-23-2C:freeradius"
      Calling-Station-Id = "00-13-02-AB-FD-0A"
      Framed-MTU = 1400
      NAS-Port-Type = Wireless-802.11
      Connect-Info = "CONNECT 11Mbps 802.11b"
      EAP-Message =
0x0222001d19001703010012 46d94ef5a81d20955db0333ed568a1c978d9
      State = 0xb49a6f49bcb87671c4117710cfb4fd3a
      Message-Authenticator = 0x5fa5c10f3006bbef7c3e48c62fe01cd3
```

- La réponse de la base d'authentification LDAP :

```
[ldap] user U00001 authorized to use remote access
[ldap] returns ok
```

- Un « **Access-Challenge** » est aussi émis par le serveur Radius pour demander soit de réémettre un « **Access-Request** » ou pour demander des informations complémentaires :

```
Sending Access-Challenge of id 131 to 192.168.1.1 port 3072
EAP-Message =
0x0123002619001703010 01b3234d6cccdea230141650972e538b5d926d5ba301cf48143790
26f
Message-Authenticator = 0x00000000000000000000000000000000
State = 0xb49a6f49bdb97671c4117710cfb4fd3a
Finished request 109.
Going to the next request
Waking up in 4.7 seconds.

rad_recv : Access-Request packet from host 192.168.1.1 port 3072 , id=132,
length=195
      User-Name = "U00001"
      NAS-Port = 0
      Called-Station-Id = "00-26-5A-B2-23-2C:freeradius"
      Calling-Station-Id = "00-13-02-AB-FD-0A"
      Framed-MTU = 1400
      NAS-Port-Type = Wireless-802.11
      Connect-Info = "CONNECT 11Mbps 802.11b"
      EAP-Message =
0x022300261900170301001b585f9dddcbd2040e2738890f46bb86e58e9c75e61fbb2a18cf0
dcc
      State = 0xb49a6f49bdb97671c4117710cfb4fd3a
      Message-Authenticator = 0x08480cc0768849a772e3b59d235cf7d2
```

- Puis un « **Access-Accept** » qui permet d'accepter la requête du client après interrogation de sa base d'authentification :

```
Sending Access-Accept of id 132 to 192.168.1.1 port 3072
      MS-MPPE-Recv-Key =
0x865535b5bb8827a0d141b4e3e2a6b8cf4fe5f0a43cf4f251f32774d2547af377
      MS-MPPE-Send-Key =
0xb9500503b6194213d5cdeac2ab4106b1983c29c21449eb8734f96cf7201e77f3
      EAP-Message = 0x03230004
      Message-Authenticator = 0x00000000000000000000000000000000
      User-Name = "U00001"
      Finished request 110.
```

IV. Conclusion

Ce projet est une solution efficace qui peut-être adaptée à toutes les entreprises qui souhaitent avoir une sécurisation de leurs infrastructure sans fil à faible cout, une gestion des utilisateurs simplifiée et adaptée aux contraintes de compétences du service administratif.

Ce projet nous a permis de mettre à profit nos compétences acquisent durant notre formation, par l'implémentation du service d'authentification Radius et du stockage des utilisateurs dans un annuaire LDAP. De plus, l'infrastructure réseau utilisée nous a familiarisé avec des sécurités de cryptages récentes comme le WPA2 /AES, ces nouvelles technologies sont nécessaires pour éviter toutes violations du système lors de tentatives malveillantes.

La mise en place d'une interface de gestion des utilisateurs nous a aidé à prendre connaissance du langage de programmation PHP pour ainsi communiquer avec l'annuaire OpenLdap via plusieurs pages Web intranet.

Référence :

- www.coagul.org/
- http://projets-gmi.univ-avignon.fr
- http://raisin.u-bordeaux.fr
- http://www.infos-du-net.com/forum/280993-8-tuto-borne-acces-wifi-authentification-radius-ldap
- http://www.commentcamarche.net/contents/php/phpldapadmin.php3
- http://www.openldap.org/
- http://php.net/manual/fr/index.php
- http://www.mail-archive.com/freeradius-users@lists.cistron.nl/msg09030.html
- http://deployingradius.com/documents/protocols/compatibility.html
- http://aternatik.org/articles-et-ressources/ldap-17/Installation-d-un-serveur-d,051
- http://www.debianadmin.com/apache2-installation-and-configuration-with-php-support-in-debian-linux.html